Sentinelcore-Ai

WHITEPAPER · INCIDENT REPORTING



The First 72 Hours: Incident Reporting under NIS2, DORA and GDPR

Every clock, every report, who to notify, and what to have ready before the incident happens.

By Harsukh Singh

Eight years in security engineering, information security governance and identity

September 2026 · sentinelcore-ai.com

Free to share with attribution

EXECUTIVE SUMMARY

One incident, several regulators, overlapping clocks

A serious cyber incident at a European organisation can trigger reporting duties under NIS2, DORA and the GDPR at the same time, each with its own authority, trigger, deadline and content. The hours after detection are the worst time to work that out.

This paper sets the obligations side by side, shows how the clocks interact, and lists what to prepare in advance so the reports are a formality rather than a scramble. It is general guidance; national transpositions of NIS2 and sector rules add detail, so confirm specifics with your competent authority and legal counsel.

The clocks at a glance



NIS2 (Article 23)

Essential and important entities must notify their CSIRT or competent authority of any **significant incident**, meaning one that has caused or can cause severe operational disruption or financial loss, or considerable damage to others. The sequence is:

- **Early warning** without undue delay and within **24 hours** of becoming aware, indicating whether the incident is suspected to be caused by unlawful or malicious acts or could have cross-border impact.
- **Incident notification** within **72 hours** of becoming aware, updating the early warning with an initial assessment, severity and impact, and indicators of compromise where available.
- **Intermediate report** on request of the CSIRT or authority.
- **Final report** within **one month** of the incident notification, with a detailed description, the likely root cause, mitigation applied and any cross-border impact; a progress report if the incident is still ongoing.

Where appropriate, entities must also inform recipients of their services who are potentially affected by a significant cyber threat about measures they can take.

DORA (Articles 17–19 and technical standards)

Financial entities classify ICT-related incidents using DORA's criteria and must report **major** incidents to their competent authority. Under the Commission's technical standards on incident reporting, the timelines are:

- **Initial notification** within **4 hours** of classifying the incident as major, and no later than **24 hours** after becoming aware of it.
- **Intermediate report** within **72 hours** of the initial notification, updated when the status changes significantly.
- **Final report** within **one month** of the latest intermediate report.

DORA also provides for voluntary notification of significant cyber threats, and requires informing clients where an incident affects their financial interests.

GDPR (Articles 33–34)

If personal data is affected, the controller must notify the supervisory authority **without undue delay and, where feasible, within 72 hours** of becoming aware of a personal data breach, unless it is unlikely to result in a risk to individuals; later notifications must explain the delay. Where the breach is likely to result in a **high risk**, affected individuals must be informed without undue delay. Processors must notify controllers without undue delay.

	NIS2	DORA	GDPR
Who	Essential & important entities	EU financial entities	Controllers (processors inform controllers)
Trigger	Significant incident	Major ICT-related incident	Personal data breach (unless unlikely to pose risk)
Recipient	CSIRT or competent authority	Competent financial authority	Data protection supervisory authority
First report	Early warning, 24h	Initial, 4h after classification (max 24h)	Notification, 72h where feasible
Follow-up	Notification 72h; final 1 month	Intermediate 72h; final 1 month	Phased information allowed

> **Lex specialis**
> For financial entities within DORA's scope, DORA's incident reporting generally takes precedence over NIS2's for ICT incidents (NIS2 Article 4 and DORA recitals). GDPR obligations still apply in parallel when personal data is involved.

Where teams lose time

- **Unclear 'awareness'.** Clocks start at awareness, not at confirmation. Define internally who can declare awareness and how it is recorded.
- **Classification by committee.** Agree the significance and major-incident criteria, with thresholds, before you need them.
- **Unknown recipients.** Keep authority portals, contacts and credentials current and tested.
- **Data scattered across tools.** Timelines, affected systems, indicators and customer impact live in the SIEM, ticketing and email. Collect them in one incident record as you go.
- **Approvals at 3 a.m.** Pre-approve templates and delegate sign-off for the first report.

Prepare now

- ☐ An incident response plan that names the reporting owner for each regime and a deputy.
- ☐ Written criteria for 'significant' (NIS2) and 'major' (DORA) incidents, and for personal data breach risk.
- ☐ Contact details and portal access for each authority, checked quarterly.
- ☐ Pre-filled templates for early warning, notifications, intermediate and final reports.
- ☐ SIEM alerts flowing into a single incident register with automatic timestamps.
- ☐ A tabletop exercise at least yearly that includes writing the actual reports against the clock.
- ☐ Management body briefed on its NIS2 Article 20 responsibilities.

How Sentinelcore-Ai helps

Sentinelcore-Ai ingests alerts from your SIEM into an incident register. When an incident is classified, the NIS2, DORA and GDPR clocks start automatically with live countdowns and reminders, report drafts are pre-filled from the incident record, and every step is time-stamped for the audit trail. Lessons learned turn into corrective actions linked to the controls they strengthen.

References

Directive (EU) 2022/2555 (NIS2), Articles 4, 20, 23 · Regulation (EU) 2022/2554 (DORA), Articles 17–19, and the Commission's regulatory and implementing technical standards on major ICT-related incident reporting · Regulation (EU) 2016/679 (GDPR), Articles 33–34 · ENISA and national CSIRT guidance on NIS2 incident notification.

About the author

Harsukh Singh has spent eight years in hands-on cybersecurity work across security engineering, information security governance, and identity and access management. That work has meant building and running information security management systems to ISO/IEC 27001:2022, auditing them against the standard, and designing identity and access controls on Microsoft Entra ID, from conditional access and privileged roles to access reviews. Harsukh founded Sentinelcore-Ai to give security and compliance teams the tooling that work called for: posture measured against vendor baselines, findings tied to risks and corrective actions, and evidence an auditor can follow.